

Dear Mr. Arthur Dent,

I appreciate you giving me this information. I have investigated whether Great New Games was required to inform anyone about the data leak in accordance with the EU General Data Protection Regulation ("**GDPR**"). I am aware that Great New Games' client database, containing names, addresses, and credit card numbers, was not encrypted, making the data accessible to the public for up to six days. However, Great New Games has no proof that any unauthorized database access has taken place.

I believe that Great New Games must inform the consumers about the data leak as well as the concerned authorities.

As per **Art. 33 para 1 s. 1 GDPR**, A personal data breach must be reported to the supervisory authority without undue delay and, if possible, no later than **72 hours (about 3 days)** after becoming aware of it, unless it is highly improbable that it would put the rights and freedoms of natural persons at danger.

According to **Art. 4 Nr. 7 GDPR**, "**controller**" is used to refer to someone who chooses the circumstances and methods used to treat a person's personal data. Any action taken on personal data or sets of personal data that results in an outcome such as collection, recording, organization, structuring, storage, adaptation or alteration is processing. Great New Games is the legal entity that decides why consumer data is stored and used. Thus, Great New Games is controller pursuant to **Art. 4 Nr. 7 GDPR**.

A breach of security resulting in the unintentional or intentional destruction, loss, alteration, disclosure, or access to personal data that is transferred, stored, or otherwise processed is known as a personal data breach, **Art. 4 Nr. 12 GDPR**. Customer information was disclosed without authorization because of the data leak, which made it publicly accessible.

The definition of "**processing**" in **Art. 4 Nr. 2 GDPR** supports this conclusion: Making personal data accessible is sufficient to qualify as processing. A data breach results from making data accessible to third parties without their consent, regardless of how the data is accessed.

If the breach of personal information is not likely to put the rights and freedoms of natural persons at danger, there is no notification requirement. There is no proof of unlawful data access by third parties. The standards pertaining to the rights and freedoms of natural persons are relaxed if the customer is likely to suffer significantly because of prospective third-party data access. One can contend that the risk to the rights and freedoms of natural persons from the data leak is unlikely because there is no proof of unlawful data access by third parties.

Credit card data, which is a PII (Personal Identifiable Information), was exposed during the data incident. Third parties might misuse personal information, resulting in identity fraud and financial loss. Great New Games must inform the supervisory authority of the personal data breach. The exception to the notification requirement outlined in **Art. 33 para. 1 s. 1 GDPR** is not applicable here.

After Great New Games learned of the personal data breach, the notification obligation must be performed within **72 hours (about 3 days)**. The essential elements of such a notification are laid out in **Art. 33, Paragraph 3 of the GDPR**.

The notice must include at least:

- Describe the nature of the personal data breach that has taken place. Describe the extent of the data breach including where possible, the categories and approximate number of data subjects concerned.
- Include the name and phone number of the data protection officer or another contact person who can provide more information.
- describe the likely consequences of the personal data breach
- indicate the steps Great New Games has taken or intends to take to resolve the personal data breach, including, as necessary, steps to lessen any potential negative impacts.

In addition, as per **Art. 33 para 5 GDPR**, Great New Games is required to keep a record of any personal data breaches, including the circumstances surrounding the breach, its consequences, and the corrective measures implemented. The supervisory authority will need access to this documentation.

Great New Games is the controller under the GDPR, and there has been a personal data breach. The controller must notify the data subject of a breach

without undue delay if the breach poses significant harm to the rights and freedoms of natural beings. Unlike what is stated in **Article 33 Paragraph 1 of the GDPR**, a notification obligation only applies where a data breach presents a serious risk to the human rights and liberties of natural persons.

The **GDPR's Recital 85** emphasizes the significance of data breach instances that may result in fraud, identity theft, and financial losses.

Additionally, Great New Games' risk analysis should consider the possibility of large fines under **Article 83 GDPR (s. below)**.

Several exclusions from the notice requirement are provided by **Art. 34 para.**

3 GDPR. There is no requirement to notify the data subject if

- The controller has put in place the necessary organizational and technical safeguards, and those safeguards were used to protect the personal information exposed in the data breach, especially those safeguards that render the information incomprehensible to anyone not authorized to access it, like encryption.
- The controller has since taken steps to make sure the high danger to data subjects' rights and freedoms mentioned in paragraph 1 is no longer likely to occur.

Notifying the affected data subjects would not require an excessive amount of effort. Great New Games is required to inform the impacted consumers of the data leak. The risk to the clients has already materialized because the customer data has already been made available to the public. According to our understanding, none of these exemptions apply.

In accordance with **Article 34 Paragraph 2 of the GDPR**, the data subject must be notified, and the notification must at a minimum include the following details:

- The title and contact information for the data protection officer, as well as any other contact information
- The personal data breach's anticipated effects
- Great New Games has done or is considering taking action to resolve the personal data breach, including, where necessary, action to lessen any potential negative effects.

According to **GDPR Article 83 Paragraph 4**, violations of the notification obligations are punishable by administrative fines. The maximum penalty is **10,000,000 EUR, or 2%** of the prior financial year's total worldwide annual turnover in the case of an undertaking, whichever is higher.

Contact me at any time if you have any more questions.

Thanks and regards,

Pranjal Sinha